Title of invention : **Software for restricting other software to be used by the rightful user only and method therefor**

Inventor: **Ho Keung, Tse.**

Software for restricting other software to be used by the rightful user only and method therefor

This is a continuation-in-part of patent application serial no. :08/587,448, filed on 12/01/95, which is still pending.

Field of the invention

The present invention relates to protection of ~~commercial~~ software, and particularly, to protection of ~~such~~ software against unauthorised use or copying.

Background of the invention

Conventionally, software protection methods for protecting commercial software products such as programs, multimedia software, distributed through a communication network, such as a telephone system, require a user computer to have a piece of hardware comprising decryption keys and system be installed therein, for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and the rightful user of that piece of software is being discouraged from copying it to someone else, by means of a psychological barrier.

It is therefore another object of the present invention is to provide a method to discourage a rightful user from copying his software to someone else.

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a sub-program for providing an Encrypted Identity (herein below referred to as EI sub-program), 2) a sub-program for authorising use of a software product (herein below referred to as AS sub-program), 3) a sub-program for authenticating user computer (herein below referred to as AC sub-program).

The central program is for managing the use of the individual sub-programs therein so that the AS sub-program can be protected from being accessed directly, thereby preventing it from being copied individually. The EI sub-program is for providing identity information(an encrypted identity) of its rightful owner for accessing a network central computer to obtain services or software products or alike in which a secure operation on a user account of that owner for payment therefor involved. The AC sub-program is for authenticating the computer on which it runs as being a particular predetermined computer, by determining the hardware and software configuration as well as hardware characteristics of that computer by software means and comparing the result with that required. The AS sub-program is for using the authentication result of the AC sub-program and the existence of the EI sub-program which being not protected against unauthorised use and being capable of being used by any user thereof, on a computer, as preconditions for authorising those software products obtained to be used on that computer.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the AS sub-program is the only sub-program which needs protection and according to the present invention, the AS sub-program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a software, i.e., the central program in which the EI sub-program exists and which can be used by an unauthorised user to provide the rightful user's

identity information for using the rightful user's account in obtaining, for eg., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI sub-program only, and the AS sub-program become an individual program which authorises the software product(s) to be used only when the EI sub-program exists in the same computer it runs and which is being determined by receiving an encrypted identity of the EI sub-program from the same.

According to a third embodiment, the EI and AS sub-programs are basically equivalent such that copying the AS sub-program by its rightful user to someone else is equivalent to copying the EI sub-program to someone else, thereby preventing the AS sub-program from unauthorised copying or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program inwhich a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

The present invention is directed to protecting software product(s) distributed through a communication network, against unauthorised copying or use, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer. And, the present invention will be described under the following headings:

1) The Central Program.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

3) The Sub-program for authorising use of a software product (AS sub-program).

4) The Sub-program for authenticating user computer (AC sub-program).

5) Other Embodiments.

1) The Central Program.

According to the first embodiment, there is provided a central program which being an executable program and can be caused to be executed a) by user by entering its filename in DOS environment, b) by a running program. FIG.1 is a block diagram of the central program, details are provided as follows :

a) If a user desires to access a network central computer through a communication link, the user has to cause the central program to be executed. The central program will request the user to enter a password to enable its operation and if the password coincidents with that required, it will be responsive to user's command(s) to send an encrypted identity of its rightful user, who should be that user, to the central computer.

This requirement of user password is necessary to prevent someone to access the central computer and use the account of the rightful user without his authorisation.

The central program will cause the EI sub-program, of which details will be described herein below, to be executed for providing an encrypted identity of the user, to the central computer. The central computer will permit the access request from the user if the encrypted identity is correct, for which details will be described in item 2 herein below.

b) When a running program desires to cause the AS sub-program to be executed, to authorise it to continue to run, it will first prepare an input parameter for indicating to the central program such a request and store the input parameter in a predetermined location in RAM, then through the use of a PC DOS service call for that purpose, cause the central program to be executed. If the central program is being enabled previously by the above-mentioned password, it will access the input parameter in the

predetermined location and from it the central program can determine that a running program is requesting for an authorisation command from the AS sub-program, and will then cause the AS sub-program to be executed. Otherwise, the central program will not cause the AS sub-program to authorise the running program to continue to run. As the password is a password for enabling use of AS sub-program, as well as the EI sub-program, the rightful user is discouraged from providing the password to someone else, in order that the someone else can use his AS sub-program.

For the case the central program is being caused by user to be executed, there will be no valid or no input parameter and the central program can thus know this fact.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

This sub-program uses the method used in IC credit card for identity authentication and in which an encrypted identity is generated.

When starts, the EI sub-program sends an access request to the central computer which in return will send back a random number. The EI sub-program will then encrypt the random number with a predetermined algorithm A1 and send the result to the central computer which will permit access if the result is identical with another result it obtained by performing the same encryption algorithm on that random number.

It should be noted that for each user, there is a corresponding respective encryption algorithm A1 for the identity authentication thereof and also that the central computer may use the encryption result received from the EI sub-program, if it being correct, as a user authorisation for payment to be made, from a user account for obtaining network services or software products or the like.

3) The Sub-program for authorising use of a software product (AS sub-program).

According to the present invention, there are 2 approaches for authorising a software product to be used :

i) by sending encrypted command to a running software program for authorising it to continue to run on a computer, in a similar manner as that mentioned above in item 2 for identity authentication. Specifically, the running software program includes in the input parameter, as mentioned above in item 1b, a random number it generated, then causes the central program to be executed. The AS sub-program, which being caused to be executed by the central program, as mentioned above in item 1b, sends the result it obtained by performing a predetermined encryption algorithm A2 on that random number, to the running software program which will accept the encrypted command and continue to run, if the result is identical to another result it obtained by performing the same encryption algorithm A2 on that random number.

It should be noted that continuous use of the software program requires continuously receiving encrypted commands.

It should also be noted that for each user, each of the software products for use on his/her computer(s) use a same respective encryption algorithm A2 and the encryption algorithm A2 being included into each such software product by the central computer at the time when the central computer is to supply the same to the user computer.

ii) by decrypting an encrypted part of a software product or a completely encrypted software product.

It should be noted that if the software product is a program, then it will be sufficient to have a part thereof to be encrypted, for preventing unauthorised copying and use, however, if the software product is an audio/visual multimedia data file, it should be more desirable to have the whole software product be encrypted.

The decryption of a part of or an entire software product takes place on a temporary copy of which in RAM, and that temporary copy should no longer exist after user finish using the software product, so as to prevent illegal copy from being made. Given by example only, FIG. 2 is a diagrammatic view of a program in RAM

space, with a part B thereof being encrypted. As seen, the AS sub-program decrypts part B and stores the result which size should be not equivalent to that of the encrypted copy, in 'part B decrypted'.

The AS sub-program then overwrites at the first location of 'part B encrypted' an instruction 'JUMP TO part B decrypted' and at the end of 'part B decrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and the decrypted part will be executed instead.

In the case of audio/visual multimedia software, the software will be decrypted a small part by a small part and each small part is decrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the AS sub-program to be executed in the manner as described above in item 1b, everytime it wants a decryption of a small part. Desirably, a newly decrypted small part will overwrite a previously decrypted one so that a whole copy of the decrypted software will not exist in RAM.

4) The Sub-program for authenticating user computer (AC sub-program).

The AC sub-program for authenticating a computer on which it runs as being a particular predetermined computer, and prevent use of protected software if the computer is not, and its operation is under control of the central program.

Specifically, when the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an unencrypted identity of the rightful user of the central program, then the AC sub-program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described hereinabove in item 3i, if the rightful user has a valid account which is not closed.

After authenticating the command, the AC sub-program determines the hardware and software configuration of the user computer, which includes, for eg., identities of peripherals such as mouse, printer, joystick, harddisk and floppy disk drive etc; characteristics of hardware such as running speed determination which is a function of CPU frequency, cache memory size etc; number and number of heads, cylinders, sectors of harddisk and locations of bad sectors therein; version number of operation system software and physical position of a particular software product including the central program in the harddisk; by skills well known to those in the art. For instance, the running speed can be determined by causing the computer to execute a test program and initializing a hardware counter to measure the time the computer has taken to finish executing the program. For another instance, the version number of the operation system may be determined by using a particular DOS service call.

The result of the determination and a status information indicative of the central program being initialized will be stored by the AC sub-program in a predetermined part of the central program in the harddisk, in the form of encrypted data. Thereafter, everytime when the central program is executed, it will first check the status information, and after determining that it is being initialized, it will perform a job as requested, as mentioned in item 1 herein above, and in addition thereto, it will also automatically cause the AC sub-program to be executed which will determine at least a part of the above-mentioned hardware and software configuration as well as hardware characteristics of the computer on which it runs, at a time, and the AC sub-program will encrypt an indication information in another predetermined part of the central program for causing the AS sub-program not to operate, if any part of the configuration/characteristics determined is not identical to the corresponding part of that it encrypted and stored previously.

In addition thereto, the AC sub-program will also reset the encrypted status information so that another initialization process will automatically take place when

the user causes the central program to be executed, and for the authorisation of which another encrypted command from the central computer will be required.

This prevents a user from deliberately adapting the central program to computer of other user(s), after closing his account.

In addition, the encrypted command from the central computer may alternatively be supplied to the user via, e.g., a telephone line, and then entered into the user computer by the user. Specifically, to request for an encrypted command, the AC sub-program generates a random number and conveys the random number to the user who in turn supplies it to the central computer by means of telephone dual tone signals, generated by entering the random number on a telephone keypad, through the telephone line, and after encrypting the random number, the central computer sends the result to the user via the same telephone line by means of a voice synthesizer.

5) Other Embodiments

According to the second embodiment, the AS sub-program is separated from the central program and become an independent program, whereas the central program comprises the EI sub-program only. The AS program is bound to the EI sub-program by requiring the AS program to operate only when the EI sub-program exists in the same computer. Specifically, the AS program when running, can cause the EI sub-program to be executed for generating an encrypted identity for the AS program to authenticate. The EI sub-program knows that this is a request for encrypted identity from the AS program, not a request from user for encrypted identity for accessing the central computer, by the method of input parameter as mentioned above in item 1b.

Further, the EI sub-program before sending the encrypted identity to the AS program, may first check the data integrity of itself by, for instance, checksum method. Alternatively, it may also be that the AS program performs the checking. And, if the checking result is that some data in the EI sub-program being altered, then in the former case, the AS will be caused to be not operable by the EI sub-program by

not sending it an encrypted identity, and in the latter case, the AS program will be caused to be not operable by itself.

According to the third embodiment, the encryption algorithms A1 and A2 that the EI and AS sub-programs use respectively for providing an encrypted identity to the central computer and for generating encrypted commands to authorise use of a software product respectively, is a same algorithm.

Thus, it would be equivalent for a rightful user to copy his EI sub-program to someone else if he copies his AS sub-program to someone else. In this case, a slight modification on the AS sub-program can make it equivalent to the EI sub-program and which involves adding a simple interface program for receiving a random number from the central computer, feeding the random number into the AS sub-program, receiving the encryption result from the AS sub-program and supplying the encryption result to the central computer, and such functions are commonly found in any network interface software. Alternatively, the A1 and A2 algorithms may be 2 different algorithms, but information representative of the A1 algorithm is being included into the AS sub-program and be accessible by user or when the AS sub-program being executed, capable of being used by AS sub-program to perform the corresponding encryption function which being user-usable.

In addition, according to another embodiment of the present invention, the software products and AS sub-program each includes an identity of its rightful user, so as to facilitate legal action against piracy. Further, the AS sub-program, when executed, will access each of the software products, by using a particular DOS service call for loading a software product stored in the computer on which it runs, from harddisk to RAM, one by one, for checking such an identity therein, if any software product is found to have an identity not identical to that of the AS sub-program, the AS sub-program will inhibit use of all software products under its control, including itself, on the computer. Such identities may be stored in a predetermined location of the software products, and is protected from being altered by having an encrypted one

stored in another location in each software product, and each of those another locations is different in different software products so that it would not be discovered and altered. And, each such software product, when executed, will automatically check the unencrypted identity stored therein against the decryption result of the encrypted one, if they are not consistent, the software product will fail to operate. The identity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the AS sub-program from mistakenly regarding a software product which stored in the computer and which being not supplied from the central computer, as a software product under its control, the central computer may further include information in a third predetermined location of each software product for indicating this fact, that is, the software product being supplied from the central computer, to the AS sub-program and each software product will not operate if when being executed, it finds that information therein being altered.